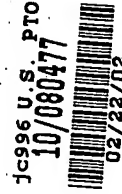


IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Richard BROWN, et al. )  
Serial No.: not yet assigned )  
Filed: Concurrently herewith ) Our Ref: B-4518 619564-1  
For: "TRUSTED COMPUTING ENVIRONMENT") Date: February 22, 2002

CLAIM TO PRIORITY UNDER 35 U.S.C. 119

Commissioner of Patents and Trademarks  
Box New Patent Application  
Washington, D.C. 20231

Sir:

[X] Applicant hereby makes a right of priority claim under 35  
U.S.C. 119 for the benefit of the filing date(s) of the  
following corresponding foreign application(s):

<u>COUNTRY</u>	<u>FILING DATE</u>	<u>SERIAL NUMBER</u>
GB	23 February 2001	0104670.5

- [ ] A certified copy of each of the above-noted patent  
application was filed with the Parent Application  
No. \_\_\_\_\_.
- [X] To support applicant's claim, a certified copy of the above-  
identified foreign patent application is enclosed herewith.
- [ ] The priority document will be forwarded to the Patent Office  
when required or prior to issuance.

Respectfully submitted,

Richard P. Berg  
Attorney for Applicant  
Reg. No. 28,145

LADAS & PARRY  
5670 Wilshire Boulevard  
Suite 2100  
Los Angeles, CA 90036  
Telephone: (323) 934-2300  
Telefax: (323) 934-0202

**THIS PAGE BLANK (USPTO)**

eu 89 463601002



INVESTOR IN PEOPLE

The Patent Office  
Concept House  
Cardiff Road  
Newport  
South Wales  
NP10 8QQ

Jc996 U.S. PTO  
10/080477

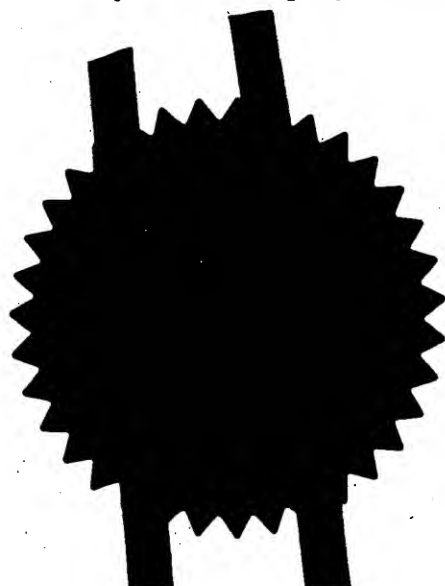


I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.



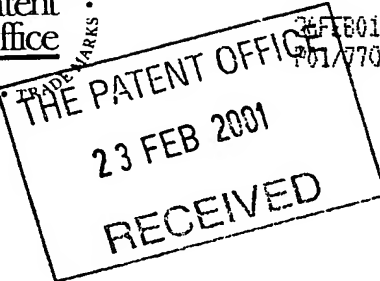
Signed

Dated

07 APR 2001

**CERTIFIED COPY OF  
PRIORITY DOCUMENT**

**THIS PAGE BLANK (USPTO)**



24 FEB 01 E609005-1 D01463  
201/7700 0.00-0104670.5

The Patent Office

Cardiff Road  
Newport  
South Wales  
NP10 8QQ

# Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

23 FEB 2001  
30006602 GB

1. Your reference

2. Patent application number  
(The Patent Office will fill in this part)

0104670.5

3. Full name, address and postcode of the or of each applicant (underline all surnames)

Hewlett-Packard Company  
3000 Hanover Street  
Palo Alto  
CA 94304, USA

Patents ADP number (if you know it)

00496588001  
Delaware, USA

If the applicant is a corporate body, give the country/state of its incorporation

4. Title of the invention **Trusted Computing Environment**

5. Name of your agent (if you have one)

Richard A. Lawrence  
Hewlett-Packard Ltd, IP Section  
Filton Road  
Stoke Gifford  
Bristol BS34 8QZ

"Address for service" in the United Kingdom to which all correspondence should be sent (including the postcode)

Patents ADP number (if you know it)

07448038001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and (if you know it) the or each application number

Country

Priority application number  
(if you know it)

Date of filing  
(day / month / year)

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application

Date of filing  
(day / month / year)

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if:

Yes

- a) any applicant named in part 3 is not an inventor, or
  - b) there is an inventor who is not named as an applicant, or
  - c) any named applicant is a corporate body.
- See note (d))

**Patents Form 1/77**

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form

Description	6
Claim(s)	2
Abstract	1
Drawing(s)	2 + 2

10. If you are also filing any of the following, state how many against each item.

Priority documents	-
Translations of priority documents	-
Statement of inventorship and right to grant of a patent (Patents Form 7/77)	1 ✓
Request for preliminary examination and search (Patents Form 9/77)	1 ✓
Request for substantive examination (Patents Form 10/77)	-
Any other documents (please specify)	Fee Sheet ✓

11. I/We request the grant of a patent on the basis of this application.

Signature   
Richard A. Lawrence

Date 22/02/01

12. Name and daytime telephone number of person to contact in the United Kingdom
- Meg Joyce Tel: 0117-312-9068

**Warning**

*After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.*

**Notes**

- If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.
- Write your answers in capital letters using black ink or you may type them.
- If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.
- If you have answered 'Yes' Patents Form 7/77 will need to be filed.
- Once you have filled in the form you must remember to sign and date it.
- For details of the fee and ways to pay please contact the Patent Office.

**TRUSTED COMPUTING ENVIRONMENT**

5

**FIELD OF THE INVENTION**

The invention relates establishing and/or maintaining a trusted computing environment. A first computing device can be said to regard a second computing device as trustworthy if the first computing device can expect the second computing device to operate or behave in a known manner.

**BACKGROUND TO THE INVENTION**

In the present context, "trust" and "trusted" are used to mean that a device or service can be relied upon to work in an intended, described or expected manner, and has not been tampered with or subverted in order to run malicious applications. A specification for trusted computing has been developed by the Trusted Computing Platform Alliance and can be found at [www.trustedpc.org](http://www.trustedpc.org).

20

A conventional trusted computing device comprises a tamper resistant tester which can test the device to ascertain if it is trustworthy. The outcome of the test can be used within the device or reported to another computing device attempting to communicate with it. An exemplary trusted component is described in the applicants co-pending International Patent Application Publication No. PCT/GB00/00528 entitled "Trusted Computing Platform", the contents of which are incorporated by reference herein. If the outcome of the test is reported to another device, then that other device can use the report to determine a trust policy vis-a-vis the device offering the report, which controls its communication with the reporting device.

30

One disadvantage of a computing environment comprised of trusted computing devices of the kind mentioned above arises where a trusted computing device becomes compromised, e.g. by a virus. The trusted computing devices in the environment do not know if the other computing devices within the environment have been compromised unless they challenge

the other computing devices to verify that they have not been compromised. The challenge-verification process can consume undesirable amounts of time and/or processing resources.

## 5 SUMMARY OF THE INVENTION

An object of the invention is the amelioration of the aforementioned disadvantage.

10 According to one aspect, the invention comprises a method of operating a trusted computing system, the method comprising providing an assessor to receive a report from, and pertaining to the trustworthiness of, a first computing device, and the assessor updating the trust policy of a second computing device in accordance with the report.

15 According to another aspect, the invention comprises an assessor for controlling a trusted computing system, the assessor comprising a receiver for receiving a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device.

20 Hence, the invention can provide an efficient way of informing computing devices within an environment about the trustworthiness of other computing devices within the environment, so as to establish or maintain a trusted computing environment. In maintaining a trusted computing environment, the invention may enable a computing device to be sure of, and keep up to date with, the level of trustworthiness of other  
25 computing devices in the environment.

In one embodiment, the report contains an assessment of the trustworthiness that has been prepared by the reporting computing device itself. In another embodiment, the report provides information about the reporting computing device that is sufficient to allow the  
30 assessor to assess the trustworthiness of the reporting computing device. Preferably, the reporting computing device comprises a trusted component which evaluates the



trustworthiness of the computing device and provides the report. The trusted component is preferably resistant to tampering and capable of applying a digital signature to the report to permit authentication of the report. The reporting computing device may be triggered to provide the report in response to a certain event or any one of a number of predetermined events. For example, the reporting computing device may be triggered to report by a request from an assessor for a trustworthiness report, or by being initialised or reset, or by the occurrence of an undesirable event (e.g. the computing device being compromised by a virus).

- 10 The assessor may, subsequent to receiving a trustworthiness report, update the trust policies of more than one computing device, one of which may be the computing device that provided the trustworthiness report.

A computing device in the context of the invention may be, for example, a computer or a peripheral (such as a scanner or printer) or other device having some data processing ability.

#### BRIEF DESCRIPTION OF THE FIGURES

By way of example only, some embodiments of the invention will now be described by reference to the accompanying drawings in which:

Figure 1 is a block diagram of a trusted computing environment; and

Figure 2 is a block diagram of an assessor.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The trusted computing environment 100 of Figure 1 comprises an assessing computer 110, or "assessor", which acts as a service provider to the computing devices in the environment, 112, 114, 116 and 118. In practice, the environment may comprise a different number of computing devices. Each computing device has at least some capacity for processing data and therefore at least some capacity for becoming untrustworthy or

affecting the trustworthiness of other computing devices with which it communicates. In this embodiment, devices 112, 114 and 116 are networked computers and device 118 is a network printer serving devices 112, 114 and 116.

- 5 Each of the computing devices 112 to 118 comprises a trusted component and a memory 122 holding a policy. A policy allows a computing device to determine the level to which it trusts other computing devices sharing the environment.

10 As an example, a policy within a computing device may list the surrounding computing devices and specify the degree to which each of them is to be trusted. In order to set the degree of trust, a policy may specify that a particular computing device is to be interacted with for all purposes, selected purposes or not at all.

15 As a further example, a policy within a computing device may specify a list of components (either software or hardware) that are untrusted. If a computing device containing such a policy finds one or more of these components in another computing device, then it can determine accordingly the degree to which it trusts that other computing device.

20 Each trusted component 120 is arranged, in a known manner, to assess the trustworthiness of the computing device with which it is associated, and to report its assessment to the assessor 110. The report may contain, for example, a decision made by the trusted component as to the trustworthiness of its host computing device, or the trusted component may simply audit its host so that the report lists the components of its host. Examples of trusted components, and the monitoring of components or processes of a host, are found in  
25 the applicants co-pending International Patent Applications as follows: Publication No. PCT/GB00/02004 entitled "Data Logging in Computing Platform" filed on 25 May 2000 and Publication No. PCT/GB00/00495 entitled "Protection of the Configuration of Modules in Computing Apparatus", filed on 15 February 2000, the contents of which are incorporated by reference.

The trusted component 120 can be arranged to be triggered to report by any of a number of events. For example, the report can be triggered by a request for a report received from the assessor 110, initialisation or resetting of the host computing device, or by some undesirable event (e.g. detection of the computing device being compromised by a known virus or the loading or addition of components unrecognised by the trusted component). Alternatively, the trusted component 120 can be arranged to make periodic reports to the assessor.

To maintain security, the trusted component 120 and the memory 122 holding the policy are incorporated in the corresponding computing device in such a manner that the trusted component 120 can perform its assessments on the computing device and yet the computing device is unable to modify the operation of the trusted component or the content of the policy. The memory 122 is arranged to accept updates to the policy that are certified by containing the digital signature of the assessor 110. Similarly, the trusted component is arranged to certify its outgoing reports with a digital signature which the assessor 110 can verify. The memory 122 containing the policy may be integrated with the trusted component 120.

As shown in Figure 2, the assessor 110 comprises a receiver 200, an updater 210, a transmitter 212 and a requestor 214. In response to being polled by the requestor 214, the receiver 200 receives the reports from the trusted components (which contain, for example, decisions on trustworthiness or component inventories), the updater 210 updates the computing devices' policies as necessary and the transmitter 212 disseminates the updated policies. Clearly it is desirable that the assessor 110 or at least relevant functions thereof are also trusted.

In the present embodiment, the assessor polls the trusted components within the computing devices 112 to 118 for trustworthiness reports. Consider the case where printer 118 has been contaminated by a virus. The report from this device alerts the assessor 110 to this fact and the assessor 110 responds by transmitting updated policies to the computing devices 112 to 118. The extent to which an updated policy curtails the extent to which the

computing device hosting the policy interacts with the affected device 118 depends on the relationship between the two computing devices. In this example, the policy of device 116 is updated to reflect that it can only send urgent print requests to printer 118 and the policies of devices 112 and 114 are updated to reflect that they are not to interact with the  
5 printer 118 or, due the continuing potential for it to be compromised by printer 118, computing device 116.

Due to the invention, a trusted computing network or environment can be established or maintained without a computing device being required to directly challenge the  
10 trustworthiness of another device when it is required to communicate with that device.

### CLAIMS

5 1. A method of operating a trusted computing system, the method comprising an assessor receiving a report from, and pertaining to the trustworthiness of, a first computing device, and the assessor updating the trust policy of a second computing device in accordance with the report.

10 2. A method according to claim 1, wherein the assessor updates the trust policies of multiple computing devices in accordance with the report.

15 3. A method according to claim 1 or 2, wherein the assessor updates policies by assessing the trustworthiness of the first computing device on the basis of information about the first computing device in the report.

4. A method according to claim 1 or 2, wherein the assessor updates policies on the basis of an assessment of the trustworthiness of the first computing device contained in the report.

20 5. A method according to any one of claims 1 to 4, wherein the assessor requests the first computing device to make the report.

25 6. A method according to any one of claims 1 to 4, wherein the first computing device is caused to report by being started-up or reset, or by an undesirable event occurring.

7. A method according to any one of claims 1 to 4, wherein the first computing device is caused to report periodically.

8. An assessor for controlling a trusted computing system, the assessor comprising a receiver for receiving a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device.

9. An assessor according to claim 8, wherein the updater is arranged to update the trust policies of multiple computing devices in accordance with the report and the transmitter is arranged to transmit the updated policies to the multiple computing devices.

10. An assessor according to claim 8 or 9, wherein the updater updates policies by assessing the trustworthiness of the first computing device on the basis of information about the first computing device in the report.

11. An assessor according to claim 8 or 9, wherein the updater updates policies on the basis of an assessment of the trustworthiness of the first computing device contained in the report.

12. An assessor according to any one of claims 8 to 11 further comprising a requestor, for requesting the report from the first computing device.

13. A system comprising an assessor for controlling a trusted computing system, the assessor comprising a receiver for receiving a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device, and the system further comprising first and second computing devices, wherein at least the first computing device comprises a reporter for sending a trustworthiness report to the assessor and at least the second computing device comprises a memory maintaining a trust policy such that the trust policy is modifiable by the transmitter.

**ABSTRACT****TRUSTED COMPUTING ENVIRONMENT**

5

A trusted computing environment 100, wherein each computing device 112 to 118 holds a policy specifying the degree to which it can trust the other devices in the environment 100. The policies are updated by an assessor 110 which receives reports from trusted  
10 components 120 in the computing devices 112 to 118 which identify the trustworthiness of the computing devices 112 to 118.

(FIGURE 1)

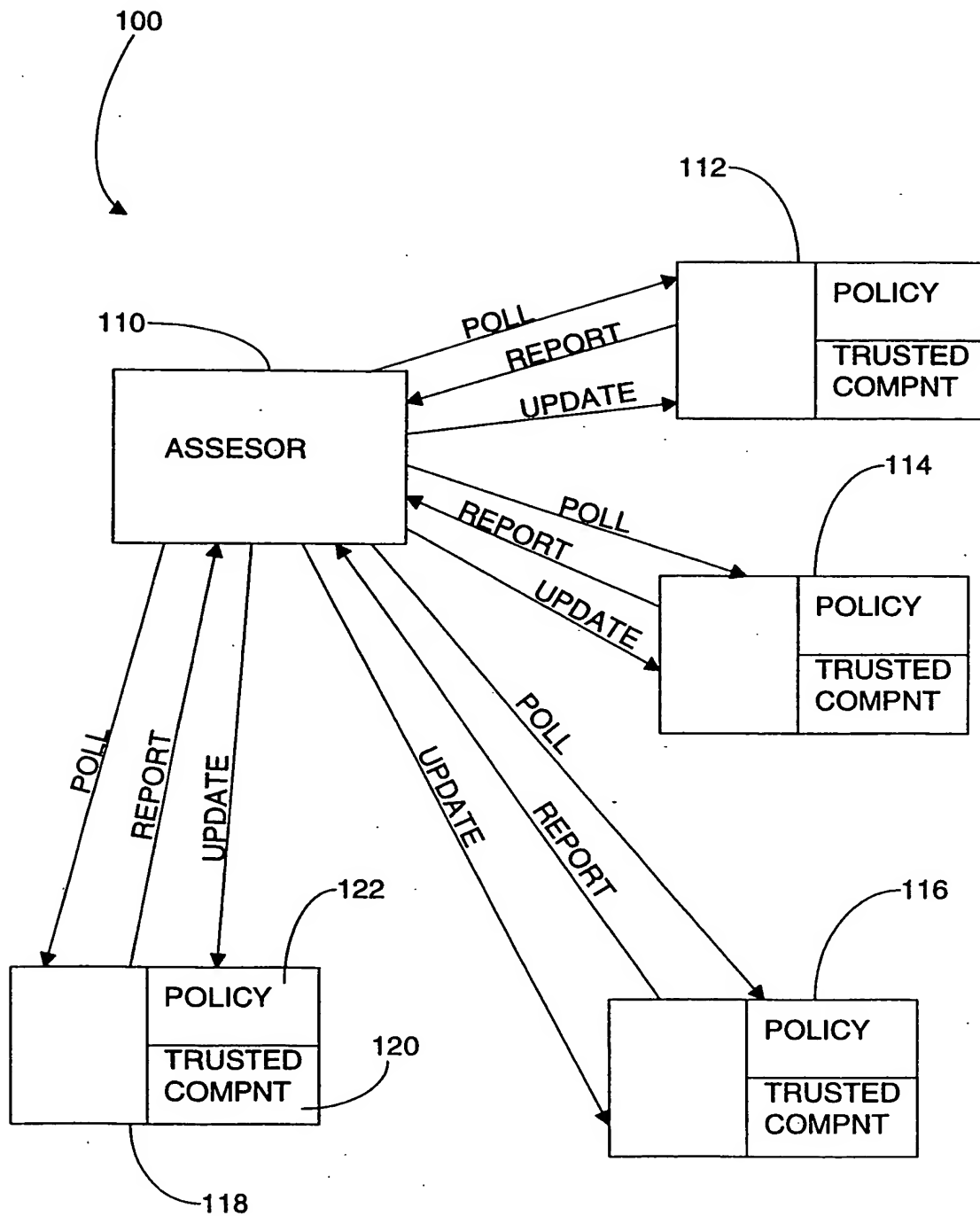


Figure 1



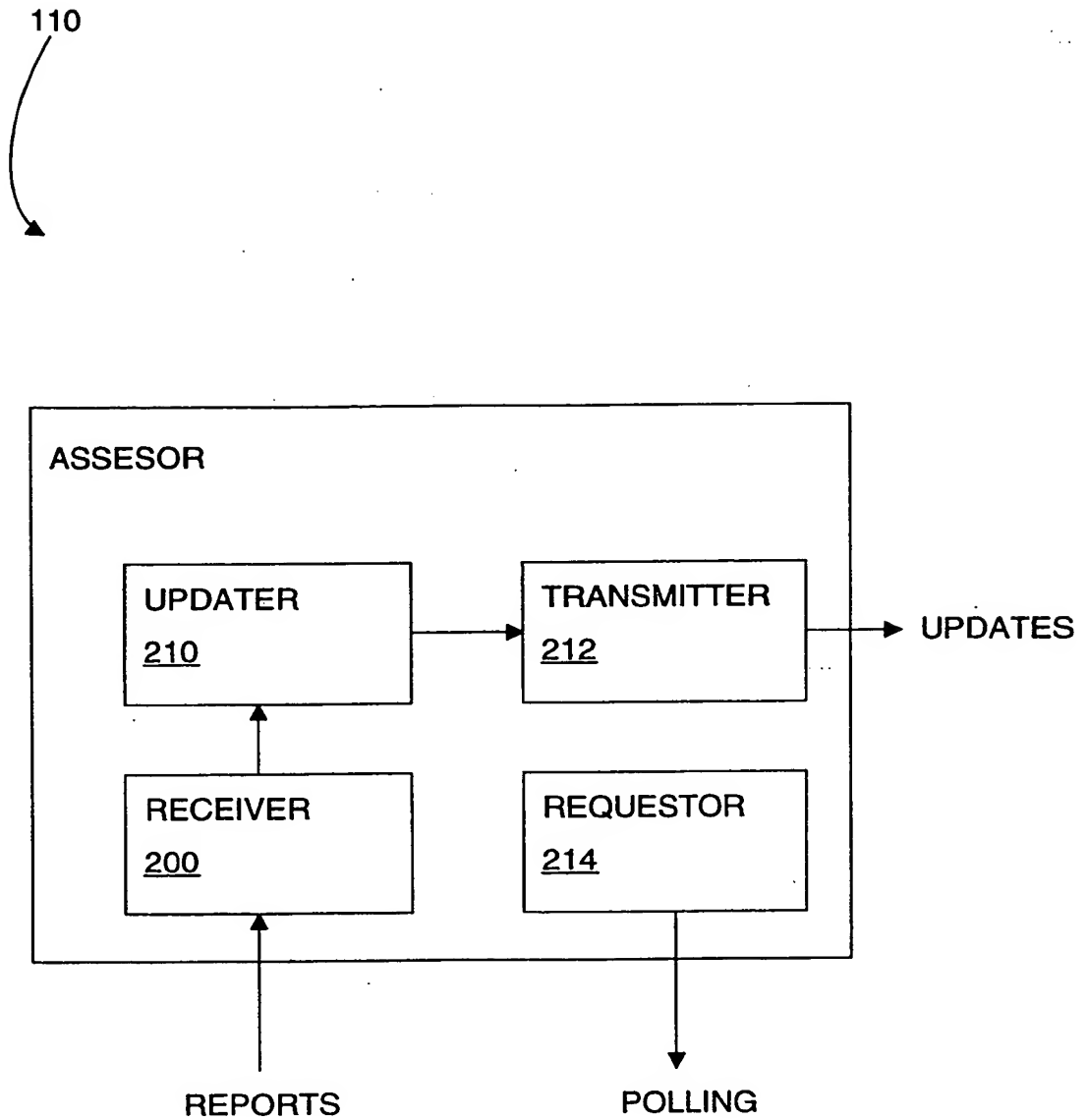


Figure 2

**THIS PAGE BLANK (USPTO,**